

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

GRACE VIVIANO, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

EMMANUEL COLLEGE,

Defendant.

Case No. _____

Judge

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Grace Viviano (“Plaintiff”) brings this Class Action Petition (“Petition”) against Defendant Emmanuel College (“Emmanuel” or “Defendant”), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels’ investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Petition against Emmanuel for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to: full names, academic transcripts, class schedules, dates of birth, student IDs, financial aid awards, financial aid payments, GPA, grades on assignments or tests (collectively, “personally identifiable information” or “PII”) and health insurance information, which is protected health information (“PHI”, and collectively with PII, “Private Information”) as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).

2. Defendant is “a Catholic, coeducational, residential, liberal arts and sciences

college situated on 17 acres in the City of Boston's Fenway neighborhood.”¹

3. Upon information and belief, former and current students, employees, and applicants for admission or employment are required to entrust Defendant with an extensive amount of their Private Information, used for Defendant's business, in order to enroll at Emmanuel or be eligible for employment. Defendant retains this information for at least many years and even after the relationship has ended.

4. On an undisclosed date, Defendant detected a cyberattack on its systems.² In response, Defendant purports to have “immediately commenced a prompt and thorough investigation.”³ As a result of its investigation, Defendant concluded—on or about January 16, 2024—that “the files removed from our network by the unauthorized actor on April 27, 2023 contain[ed]” Plaintiff's and Class Members' Private Information.⁴

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and approximately 89,000 other individuals' information.⁵

6. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. Defendant failed to adequately protect Plaintiff's and Class Members Private

¹ <https://www.emmanuel.edu/about>

² The “Notice Letter”. A sample copy is available at <https://apps.web.main.gov/online/aewviewer/ME/40/63bfe061-8381-4397-b07b-2a78d22f5785.shtml>

³ *Id.*

⁴ *Id.*

⁵ According to the report submitted to the Office of the Maine Attorney General, 89,064 individuals were impacted. See <https://apps.web.main.gov/online/aewviewer/ME/40/63bfe061-8381-4397-b07b-2a78d22f5785.shtml>

Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect students' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence, at a minimum, and violates federal and state statutes.

9. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and

adequate measures to protect the Private Information.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

12. Plaintiff Grace Viviano is a natural person, resident, and a citizen of Boston, Massachusetts.

13. Defendant Emmanuel College is a Massachusetts college with its principal place of business in Boston, Massachusetts.

JURISDICTION AND VENUE

14. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant,⁶ there are more than 100 putative class members, and the amount in controversy exceeds \$5 million exclusive of interest and costs.

⁶ According to the report submitted to the Office of the Maine Attorney General, 2,899 Maine residents were impacted in the Data Breach. See <https://apps.web.main.gov/online/aeviewer/ME/40/63bfe061-8381-4397-b07b>

15. This Court has general personal jurisdiction over Defendant because it maintains its principal place of business in this District, regularly conducts business in Massachusetts, and has sufficient minimum contacts in Massachusetts.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1331(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District

FACTUAL ALLEGATIONS

Defendant's Business

17. Defendant is "a Catholic, coeducational, residential, liberal arts and sciences college situated on 17 acres in the City of Boston's Fenway neighborhood."⁷

18. Plaintiff and Class Members are or were students and/or student applicants at Emmanuel or provided Defendant with the relevant Private Information for some other purpose (e.g., employment or application for employment or study).

19. To enroll in classes or other programs at Defendant, Plaintiff and Class Members were required to provide sensitive and confidential Private Information, including but not limited to: their names, dates of birth, and other sensitive information.

20. Upon information and belief, Defendant made promises and representations to its students, including Plaintiff and Class Members, that the Private Information collected from them as a condition of enrollment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

^{2a78d22f5785.shtml}

⁷ <https://www.emmanuel.edu/about>

21. Indeed, Defendant's Privacy Policy provides that: "Emmanuel College is committed to the privacy of all visitors—including alumni, students, faculty, staff and friends[.]”⁸

22. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their Private Information.

23. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

24. Defendant had obligations created by FTC Act, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

25. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

The Data Breach

26. On or about January 31, 2024, Defendant began sending Plaintiff and other victims of the Data Breach an untitled letter (the "Notice Letter") informing them that:

We are writing with important information regarding a data security incident that involved your personal information.

...

Upon learning of the issues, we contained the threat, notified law enforcement and

⁸ <https://www.emmanuel.edu/copyright-and-privacy-policy#:~:text=The%20College%20will%20use%20your,processing%20and%20completing%20academic%2C%20financial>

immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following a forensics investigation and complex manual review, we discovered on January 16, 2024, that the files removed from our network by the unauthorized actor on April 27, 2023 contain your personal information. That at-risk files contained some of your personal information, including your full name along with your Academic Transcript, Class Schedule, Date of Birth, Student ID, Financial Aid Award, Financial Aid Payment, GPA, Grades on Assignment or Test, Health Insurance Policy #/Subscriber#.⁹

27. Omitted from the Notice Letter were the date that Defendant detected the Data Breach, any explanation as to why Defendant failed to notify Plaintiff and Class Members of the Data Breach for *more than nine months* after the cyberattack's occurrence, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

28. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

30. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their

⁹ Notice Letter.

names, dates of birth, PHI, and other sensitive information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

31. Plaintiff furthers believe that her Private Information and that of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information , such as encrypting the information or deleting it when it is no longer needed.

33. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹⁰

34. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

¹⁰ How to Protect Your Networks from RANSOMWARE, at 3, available at: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹¹

35. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management

¹¹ *Id.* at 3–4.

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;
- Include IT Pros in security discussions
- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹²

36. Given that Defendant was storing the Private Information of its current and former students, employees, student applicants, and employee applicants, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

37. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of more than eighty thousand individuals,

¹² See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

including that of Plaintiff and Class Members.

Emmanuel Acquires, Collects & Stores Plaintiff's and the Class's Private Information

38. Defendant has historically acquired, collected, and stored the Private Information of Plaintiff and Class Members.

39. As a condition to enroll, apply for enrollment, or obtain employment at Emmanuel, Plaintiff and Class Members are required to give their sensitive and confidential Private Information to Defendant. Defendant retains this information even after the relationship has ended and Defendant is no longer required to retain this information.

40. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

41. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

42. Upon information and belief, Defendant made promises and representations to its students and employees, including Plaintiff and Class Members, that the Private Information collected from them as a condition of enrollment and/or their employment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

43. Indeed, Defendant's Privacy Policy provides that: "Emmanuel College is committed to the privacy of all visitors—including alumni, students, faculty, staff and

friends[.]”¹³

44. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

45. Defendant’s negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk because Educational Institutions in Possession of Private Information are Particularly Susceptible to Cyber Attacks

46. Defendant’s data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information, like Defendant, preceding the date of the breach.

47. Data breaches, including those perpetrated against educational institutions that store Private Information in their systems, have become widespread.

48. In the third quarter of the 2023 fiscal year alone, 7,333 organizations experienced data breaches, resulting in 66,658,764 individuals’ personal information being compromised.¹⁴

49. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they

¹³ <https://www.emmanuel.edu/copyright-and-privacy-policy#:~:text=The%20College%20will%20use%20your,processing%20and%20completing%20academic%2C%20financial>

¹⁴ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/>

collected and maintained would be targeted by cybercriminals.

50. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are “attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”¹⁵

51. Additionally, as companies became more dependent on computer systems to run their business,¹⁶ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.¹⁷

52. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

53. Defendant knew and understood unprotected or exposed Private Information in the custody of educational institutions, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

¹⁵ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newletter&utm_medium=email&utm_campaign=consumerprotection

¹⁶<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

¹⁷ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

54. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

55. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information .

56. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to more than eighty thousand individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

57. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

58. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

59. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it

entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

60. That Defendant is encouraging its current and former students and other personnel to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals are subject to a substantial and imminent threat of fraud and identity theft.

61. As an educational institution in custody of students', employees', and employee applicants' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."¹⁸ The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."¹⁹

63. The PII of individuals remains of high value to criminals, as evidenced by the

¹⁸ 17 C.F.R. § 248.201 (2013).

¹⁹ *Id.*

prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.²⁰

64. For example, Personal Information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²¹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²²

65. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”²³

66. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (e.g., patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient’s complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a “cyber black market” exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

²⁰ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>

²¹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>

²² *In the Dark*, VPNOversview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

²³ *Medical I.D. Theft*, EFraudPrevention

<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).

67. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.²⁴ Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.²⁵ In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.²⁶

68. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.²⁷

69. “Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,” reported Pam Dixon, executive director of World Privacy Forum. “Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief’s activities.”²⁸

70. A study by Experian found that the average cost of medical identity theft is “about \$20,000” per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.²⁹ Almost half of medical

²⁴ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last accessed July 24, 2023).

²⁵ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed July 24, 2023).

²⁶ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/> (last accessed July 24, 2023).

²⁷ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last accessed July 20, 2021)

²⁸ Michael Ollove, “The Rise of Medical Identity Theft in Healthcare,” Kaiser Health News, Feb. 7, 2014, <https://khn.org/news/rise-of-identity-theft/> (last accessed July 24, 2023).

²⁹ See Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar. 3, 2010), <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last accessed July 24, 2023).

identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.³⁰

71. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—PHI, dates of birth, and name.

72. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”³¹

73. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

74. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once

³⁰ *Id.*; see also *Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/> (last accessed July 24, 2023).

³¹ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>

stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³²

Defendant Fails to Comply with FTC Guidelines

75. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.³³

77. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.³⁴

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

³² Report to Congressional Requesters, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf>

³³ Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

³⁴ *Id.*

complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect student data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. These FTC enforcement actions include actions against educational institutions, like Defendant.

81. Defendant failed to properly implement basic data security practices.

82. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to its students’, employees’, and other personnel’s Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

83. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its students, employees, and other personnel. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

84. As noted above, experts studying cyber security routinely educational institutions in possession of Private Information as being particularly vulnerable to cyberattacks because of

the value of the Private Information which they collect and maintain.

85. Several best practices have been identified that a minimum should be implemented by educational institutions in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

86. Other best cybersecurity practices that are standard in the higher education industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

87. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. These foregoing frameworks are existing and applicable industry standards in the higher education industry, and upon information and belief, Defendant failed to comply with at

least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

89. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft

90. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

91. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

92. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

93. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

94. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victims.

95. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.³⁵

³⁵ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule

96. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

97. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’s and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

98. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiff and the other Class Members.

99. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

100. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsongsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsongsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsongsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-)

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

101. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

102. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter, instructs Plaintiff and Class Members to take the following measures to protect themselves: “you should always remain vigilant in reviewing your financial account statements and credit reports on a regular basis and report any fraudulent or irregular activity immediately.”³⁶

103. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft protection services offered by Defendant, changing passwords and resecuring their own computer networks, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

104. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the

³⁶ Notice Letter.

damage to their good name and credit record.”³⁷

105. Plaintiff’s mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

106. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁸

Diminution of Value of Private Information

107. PII and PHI are valuable property rights.³⁹ Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

108. Sensitive PII can sell for as much as \$363 per record according to the Infosec

³⁷ See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

³⁸ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (“GAO Report”).

³⁹ See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

Institute.⁴⁰

109. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴¹

110. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.^{42,43} Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁴⁴

111. Theft of PHI is also gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”⁴⁵

112. As a result of the Data Breach, Plaintiff’s and Class Members’ Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

⁴⁰ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>

⁴¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>

⁴² <https://datacoup.com/>

⁴³ <https://digi.me/what-is-digime/>

⁴⁴ Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqs.html>

⁴⁵ *Medical I.D. Theft*, EFraudPrevention

<https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.> (last visited Nov. 6, 2023).

113. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change, e.g., PHI, dates of birth, and names.

114. The fraudulent activity resulting from the Data Breach may not come to light for years.

115. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

116. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

117. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s network, amounting to over eighty thousand individuals’ detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

118. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant’s failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable & Necessary

119. Given the type of targeted attack in this case, the sophisticated criminal activity, and the type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims’ names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

120. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

121. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁴⁶ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as dates of birth).

122. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

123. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach.

⁴⁶ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

Loss of Benefit of the Bargain

124. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for educational services or accepting employment from Defendant under certain terms, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying, or being paid less, for services and data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services and/or employment positions that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Grace Viviano's Experience

125. Plaintiff Viviano is a former Emmanuel student and employee, attending classes at Defendant from approximately 2018 through 2022 and working at Defendant from approximately 2018 through 2021.

126. In order to enroll at Emmanuel and/or obtain employment at Emmanuel, she was required to provide her Private Information to Defendant, including her name, date of birth, and other sensitive information.

127. At the time of the Data Breach—on or around April 27, 2023—Defendant retained Plaintiff's Private Information in its system.

128. Plaintiff Viviano is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

129. Plaintiff Viviano received the Notice Letter, by U.S. mail, directly from

Defendant, dated January 31, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her full name, academic transcript, class schedule, date of birth, student ID, financial aid award, financial aid payment, GPA, grades on assignment or test, health insurance policy #/subscriber#.

130. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff to "remain vigilant in reviewing your financial account statements and credit reports on a regular basis and report any fraudulent or irregular activity immediately[,"]⁴⁷ Plaintiff made reasonable efforts to mitigate the impact of the Data Breach including, but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft protection services offered by Defendant, changing passwords and resecuring her own computer network, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

131. Plaintiff suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which:

⁴⁷ Notice Letter.

(a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

132. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

133. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

134. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

135. Plaintiff Viviano has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

136. Plaintiff brings this action on behalf of herself and all other persons similarly situated.

137. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

Nationwide Class

All persons in the United States whose Private Information was compromised as a result of the Data Breach, for which Defendant provided notice in January 2024 (the "Class").

138. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

139. Plaintiff hereby reserves the right to amend or modify the class definition with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification.

140. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. At least 89,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine's Attorney General's Office.⁴⁸ The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

141. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

⁴⁸

<https://apps.web.main.gov/online/aeviewer/ME/40/63bfe061-8381-4397-b07b-2a78d22f5785.shtml>

- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;
- h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant was unjustly enriched;
- k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

142. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach.

143. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent

and experienced in litigating class actions, including data privacy litigation of this kind.

144. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

145. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

146. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

147. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues

include, but are not limited to:

- a. Whether Defendant failed to timely notify the public of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

148. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

149. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

150. Defendant required Plaintiff and Class Members to submit sensitive, non-public, personal information in order to enroll in one of Defendant's classes or programs or be eligible for employment.

151. Defendant's duty of care to use reasonable security measures arose as a result

of the special relationship that existed between Defendant and the individuals that entrusted their Private Information to Defendant. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from the Data Breach.

152. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to design, implement, and monitor systems, policies, and processes by which it could reasonably prevent and detect a breach of their security systems in a reasonably expeditious period of time.

153. Defendant had a duty to use reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

154. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their Private Information in accordance with industry standards concerning data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass.

155. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

156. Defendant owed a duty to timely and accurately disclose to Plaintiff and Class

Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

157. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

158. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information . The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

159. The breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches generally and in the higher education industry.

160. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

161. Plaintiff and the putative class members had no way to protect themselves from the damage Defendant is responsible for.

162. The imposition of a duty of care on Defendant to safeguard the Private Information it maintained is appropriate because any social utility of Defendant's conduct—of which little, if any, exists—is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

163. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

164. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the Private Information.

165. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Breach Of Implied Contract
(On Behalf of Plaintiff and the Class)

167. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

168. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for enrolling in classes, applying for enrollment, or obtaining employment at Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information and to destroy any Private Information that it was no longer required to maintain.

169. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant on the other, is demonstrated by their conduct and course of dealing.

170. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

171. In accepting the Private Information of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

172. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including the FTC Act, and were consistent with industry standards.

173. Plaintiff and Class Members paid money and/or provided their labor to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

174. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

175. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

176. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

177. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information or to destroy it once it was no longer necessary to retain the Private Information.

178. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

179. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

180. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

181. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

182. Plaintiff brings this claim in the alternative to the breach of implied contract claim above.

183. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their Private Information and paid money and/or provided labor to Defendant and/or its agents in connection with their admission applications and/or employment at Defendant, and in so doing, provided Defendant with their Private Information based on the understanding that the benefits derived therefrom would, in part, be used to fund adequate data security. In exchange, Plaintiff and Class Members should have received from Defendant the educational services and/or employment position that were the subject of the transaction and have their Private Information protected with adequate data security.

184. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

185. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information and instead directed those funds to its own profit. Instead of providing a reasonable

level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

186. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and Class Members.

187. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

188. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

189. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

190. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

191. Defendant obtained a benefit from Plaintiff and Class Members by fraud and/or the taking of an undue advantage, in that it misrepresented and omitted material information concerning its data security practices when Plaintiff and Class Members relied upon it to

safeguard their Private Information against foreseeable risks.

192. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant or obtained educational services and/or employment at Defendant.

193. Plaintiff and Class Members have no adequate remedy at law.

194. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) statutory damages; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

195. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injuries and/or harms.

196. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 1. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 2. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;
 3. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court

reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

4. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;
5. Prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;
6. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
7. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
8. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
9. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

10. Requiring Defendant to conduct regular database scanning and securing checks;
11. Requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;
12. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
13. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
14. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

15. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect herself; and
 16. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and
 17. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
 - F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;
 - G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
 - H. For an award of punitive damages, as allowable by law;
 - I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
 - J. Pre- and post-judgment interest on any amounts awarded; and
 - K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: February 15, 2024

Respectfully submitted,

/s/ Randi Kassan

Randi Kassan

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

100 Garden City Plaza, Suite 500

Garden City, NY 11530

Telephone: (212) 594-5300

rkassan@milberg.com

David K. Lietz*

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, PLLC

5335 Wisconsin Avenue NW, Suite 440

Washington, D.C. 20015-2052

Telephone: (866) 252-0878

Facsimile: (202) 686-2877

dlietz@milberg.com

Counsel For Plaintiff and

The Proposed Class

**Pro Hac Vice* application forthcoming